SAI360
RISK FROM EVERY ANGLE

How to Turn Operational Risk Management into a Strategic Advantage with Technology



Table of Contents

Introduction 3

Managing the Full Risk Lifecycle with Technology 4

Key Considerations for Success 6

3 Ways ORM Can Be Your Competitive Advantage 7

From Fragmentation to Integration 8

Introduction

In a recent paper, Best Practices for Managing Operational Risk in 2026, we explored the evolving frameworks and regulatory expectations reshaping operational risk management (ORM). While global rulemakers have made tremendous progress in providing robust guidelines for firms to follow, the challenge lies in translating these requirements into bullet-proof processes.

Most organizations understand ORM expectations at the framework level, but struggle to implement comprehensive controls in practice. Often held back by fragmented or legacy systems, consistently accessing and analyzing the correct data across complex, siloed environments is a persistent challenge. The true test is functional, and many continue to fall short.

In 2023, materialized losses from new operational risk events in the European financial services sector alone totaled EUR 17.5 billion, a ~27% increase from the previous year, approaching the pandemic-era peak of EUR 18.7 billion (2021).[1]

Competition is fiercer than ever. In an increasingly borderless world, pressure to innovate, scale, and succeed transcends industry boundaries. Firms' ORM frameworks need to match their commercial ambition. This paper explores how technology can bring operational risk management to life, turning what often feels like a burdensome compliance exercise into a valid driver of agility, resilience, and competitive advantage.

1. https://www.eba.europa.eu/publications-and-media/publications/operational-risks-and-resilience-0?utm_source=chatgpt.com

Managing the Full Risk Lifecycle with Technology

Managing operational risk with technology means moving beyond static, reactive processes into proactive, data-driven, and continuous oversight. This enables firms to better anticipate and respond to risk in real time, rather than relying on backward-looking assessments or episodic reviews.

1. Enhanced Visibility with Data Integration

Risk quantification remains challenging due to fragmented data sources across the enterprise. Technology helps overcome this by breaking down silos and integrating risk assessments, control testing results, key risk indicators (KRIs), audit findings, incident logs, and third-party data into a unified view. This is typically achieved through data integration pipelines or ETL (extract, transform, load) frameworks that normalize and correlate heterogeneous data points. Advanced APIs and event-driven architectures enable real-time ingestion and cross-referencing of structured and unstructured risk signals from disparate systems.

No organization operates in a vacuum, so risk managers must also consider how the business interacts with its environment and how this affects the firm's risk posture. Novel solutions can ingest and translate raw, unstructured external signals into structured, actionable insight. Practically speaking, this involves systematically monitoring sources like public news, social media, regulatory updates, social media platforms, and even the dark-web for indicators of emerging operational risk.

Contextualization is essential, not just to reduce noise, but to understand how external developments impact your organization's risk profile in relation to its industry geography and strategic objectives. It also helps identify when one type of risk may evolve into another, supporting more proactive and connected risk management.

The Role of Artificial Intelligence in External Risk Visibility

Artificial intelligence (AI) has significantly enhanced how firms monitor external risk at scale. Thousands—if not millions—of potentially relevant data points emerge daily across sources. Manually processing this volume is infeasible, making AI essential for real-time visibility into emerging threats.

Advanced models can distinguish between general background noise and early warning signs of material risk. For example, a surge in negative sentiment may be immaterial, but a shift toward coordinated action, such as a boycott, should be flagged and escalated. AI helps filter and prioritize such signals across categories, including reputational, regulatory, and cyber risk.

Beyond detection, AI also supports risk analysis by mapping how external events evolve and propagate. A reputational issue may trigger regulatory scrutiny or affect financial performance. By surfacing these interdependencies, AI enables firms to respond more quickly to cascading threats.

2. Data-Driven Risk Scoring

Risk scoring engines enable firms to maximize the value of ingested data, delivering more accurate assessments as additional, relevant inputs are incorporated. These engines use statistical models, machine learning, or rule-based logic to support more granular, consistent, and objective risk evaluations. Using configurable scoring algorithms and weightings facilitates automatic risk rating by likelihood and impact, adjusted dynamically as new data flows in.

Natural language processing (NLP) can enhance scoring models by extracting sentiment and contextual insights from qualitative sources like audit reports or loss event narratives. This creates a multidimensional, data-driven view of operational risk that captures both existing and emerging exposures more precisely.

3. Dynamic Threshold Monitoring

While risk scoring provides a foundation, dynamic threshold monitoring enables firms to act on those insights in real time. Traditional controls often rely on static thresholds and periodic assessments, but with more data now available, the emphasis is shifting toward continuous risk sensing and proactive intervention.

Dynamic monitoring involves testing internal controls and performance metrics against evolving risk indicators to detect early signs of stress. Crucially, this approach allows firms to track how close specific risks are to breaching defined tolerance or appetite levels, moving from reactive to anticipatory risk management.

4. Real-Time Risk Reporting

Once risks are continuously scored and tracked against predefined thresholds, firms can generate live dashboards and automated alerts that reflect the current risk state, rather than a historical snapshot.

Technology enables this by aggregating structured and unstructured data across business units, validating it in real time, and surfacing insights through configurable reporting layers. Risk signals that once took weeks to detect through manual review can now be escalated instantly to the relevant teams. This capability is critical for operational resilience, particularly when responding to time-sensitive threats such as system outages, cyberattacks, or third-party failures.

As explored in the previous paper, emerging regulatory frameworks place additional pressure on firms to report incidents swiftly and transparently.[2] Major incidents must be reported within 24 hours of detection, followed closely by more detailed updates within 72 hours, and comprehensive reports within the month. Structure and traceability are essential to maintain compliance under tighter reporting timelines, and technology is key in automating the capture, classification, and escalation of incidents and maintaining a real-time, auditable trail of risk data.

A Note on Generative AI

Generative AI has grown popular amongst the risk management community. Large language models, in particular, excel at processing and synthesizing unstructured data, regulatory texts, internal policies, risk assessments, model documentation, etc.

The appeal lies in their ability to accelerate and enhance risk assessment workflows. Instead of manually reviewing lengthy documents, risk professionals can use generative AI to extract relevant insights, identify gaps, flag inconsistencies, and even suggest remediation measures, all within seconds. This supports faster, more consistent, and better-informed decision-making.

Some institutions are already applying generative AI to automate aspects of control design, monitoring, and incident detection. Others are experimenting with its use to draft risk and control self-assessments (RCSAs) or to evaluate the quality and completeness of existing ones. In these scenarios, generative AI acts as a force multiplier, augmenting human judgment, reducing manual workload, and enabling more responsive operational risk oversight.[3] [4]

2. https://www.sai360.com/resources/grc/best-practices-managing-operational-risk-in-2025-whitepaper
3. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/how-generative-ai-can-help-banks-manage-risk-and-compliance
4. Generative AI implementation must be considered with risks in mind: these include (but are not limited to) bias, explainability, malicious use, security, and data integrity and privacy.

Key Considerations for Success

Usability Matters

User experience (UX) is an underestimated success factor in tech-enabled risk programs. ORM is a team sport, involving many stakeholders beyond the risk office. Business unit managers need to update risk assessments, IT staff need to log incidents, and executives need to review dashboards. If the software is cumbersome or slow, these users will resist using it, leading to poor adoption and incomplete data.

Common pitfalls include complex, unintuitive screens; confusing workflows; and a lack of role-based personalization. A risk system touches users with varying skill levels – from a front-line manager who might only log in occasionally to update an action, to a power user in the risk team who lives in the system daily. The interface needs to cater to both. Best-in-class solutions focus on clean, uncluttered design and role-based views.

Tailored by Design, Not Bespoke By Build

Every organization has a unique view of operational risk. Regulations have helped standardize the ORM process, but there will always be a degree of proportionality in how the rules are applied. This reflects each firm's structures, operating environments, and subsequent risk profiles, which can differ immensely, even among close competitors.

This also recognizes that ORM processes are not static and may change with time, upon the release of new products, or upon entry into new jurisdictions. Any tool you implement must adapt to the business's needs. Historically, achieving this meant expensive customization—hiring developers to write custom code or scripts to modify off-the-shelf GRC software. However, the downside of bespoke builds is significant: long implementation times, high costs, difficulty upgrading the software, and heavy reliance on IT or vendors for every little change.

Modern risk platforms integrate with your existing tech, and they're built to be highly configurable by end-users or administrators, often now without writing code. Through point-and-click interfaces, an admin can define the company's risk taxonomy (e.g., what risk levels to use, what categories), create custom fields or forms, adjust workflows, and set role-based permissions.

3 Ways ORM Can Be Your Competitive Advantage

The culmination of tech-enabled operational risk management is a living risk profile that is continuously updated, accessible across the organization, and actionable at both strategic and operational levels. This dynamic view allows leadership to make informed decisions, allocate resources effectively, and confidently demonstrate risk governance to regulators and stakeholders.

1. Agile Decision Making

When risk data is integrated and accessible, executives can make faster, more informed decisions. Visibility is the foundation of optimization—only when you can see your risks can you manage and leverage them effectively. This enables calculated risk-taking, grounded in real-time insights from risk systems, eliminating the need for guesswork.

Consider just a few of the questions that come with market expansion: Are we ready to enter a new jurisdiction? How do the operational risks compare? Are regulatory expectations around ORM more stringent? Are our internal controls robust enough, or are we exposing ourselves to unnecessary risk?

The same questions apply when adopting new technologies or launching new products—AI, for example. Have we implemented the proper controls to manage AI-related risks? Is our security framework sufficient?

This level of insight enables confident, risk-informed go/no-go decisions. Organizations that excel in this can capitalize on opportunities others avoid because they trust their risk intelligence and the strength of their contingency planning.

2. Build Customer Trust and Brand Reputation

Our last eBook highlighted the broad social impact of the Barclays Bank outage in the UK. It was not the first incident of its kind and certainly will not be the last. Every disruption, whether a service outage, data breach, or supply chain failure, gradually erodes customer trust. Social media amplifies these events in real time, turning localized issues into reputational crises.

But the reverse is also true. Organizations responding quickly and transparently during incidents can preserve trust and strengthen their reputation. Firms that continue to serve customers effectively through disruption are seen as dependable. Reliability becomes a key differentiator in a competitive marketplace where switching barriers are low.

As a result, resilience is becoming part of the brand. Some companies now actively promote their strong risk management and business continuity capabilities as part of their value proposition. ORM used to be hidden in the back office; now, it's in the boardroom and even marketing material because stakeholders care.

3. Compliance

Global regulators, from the FCA and PRA in the UK to counterparts in the US and EU, increasingly expect firms to demonstrate resilience in action, not just on paper. Firms that can produce data-driven evidence of their risk management effectiveness – via the kind of tech-enabled reporting we've discussed – will find regulatory exams more straightforward, avoiding potentially crippling repercussions.

Recent regulatory frameworks underline the rising stakes:

- **Digital Operational Resilience Act:** Up to 2% of annual global turnover for financial institutions and €5 million for critical third-party providers, as well as daily fines, individual liability, reputational damage, and additional sanctions such as public reprimands or suspension of authorisation.
- **Network and Information Security Directive 2:** Essential entities face fines of up to €10 million or 2% of global turnover, alongside non-monetary penalties such as compliance orders and public disclosures. Directors are personally accountable for compliance, with EU member states empowered to enforce sanctions, including individual liability.

Ultimately, turning risk management into a strategic advantage means shifting the mindset from "risk as overhead" to "risk as foresight." Risk management must move from a reactive, after-the-fact cost center to a proactive business partner. Doing so helps the organization choose what risks to take in pursuit of reward (strategic risk-taking) and how to fortify against risks that offer no upside (pure operational hazards).

From Fragmentation to Integration

Fragmentation has long been one of the most significant obstacles to effective ORM. It is not uncommon for organizations to use separate tools for operational risk assessment, third-party assessments, training, and incident response. This “technology sprawl” creates silos that hinder effective risk oversight and issues can slip through the cracks, surfacing only at the point at which they escalate into incidents, which, by most accounts, is too late.

The answer lies in integration. By consolidating risk activities into a single platform, firms gain enterprise-wide visibility, real-time insights, and a consistent, actionable risk picture across the business. Instead of reacting to problems, they can anticipate and prevent them.

This level of integration is being achieved today through platforms like **SAI360,** which are helping risk teams shift from fragmented processes to unified, forward-looking risk strategies. As firms move to embed resilience and agility into their operations, integrated platforms are essential.

Our unified approach to risk sets us apart

Today’s complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform that spans the entire risk and compliance spectrum.

- Whistleblower and Case Management
- Ethics & Compliance Training
- Policy Management
- Conflicts of Interest
- Incident Management
- Regulatory Compliance
- Regulatory Obligations
- Horizon Scanning
- Enterprise & Operational Risk Management
- Third-Party Risk
- Internal Audit
- Internal Controls
- IT Risk
- Business Continuity
- Vendor Risk Management